

SUMS AND DIFFERENCES ALONG HAMILTONIAN CYCLES

VSEVOLOD F. LEV

ABSTRACT. Given a finite abelian group G , consider the complete graph on the set of all elements of G . Find a Hamiltonian cycle in this graph and for each pair of consecutive vertices along the cycle compute their sum. What are the smallest and the largest possible number of sums that can emerge in this way? What is the expected number of sums if the cycle is chosen randomly? How the answers change if an orientation is given to the cycle and differences (instead of sums) are computed? We give complete solutions to some of these problems and establish reasonably sharp estimates for the rest.

1. INTRODUCTION

For a finite abelian group G , by $\mathcal{C}(G)$ we denote the set of all Hamiltonian cycles in the complete digraph on the vertex set G ; thus, $\mathcal{C}(G)$ is empty if G is trivial and $|\mathcal{C}(G)| = (|G| - 1)!$ otherwise. Given a cycle $C \in \mathcal{C}(G)$, label each edge $(g_1, g_2) \in C$ with the sum $g_1 + g_2$ and consider the set $S(C) \subseteq G$ of all labels along C . Now let

$$\begin{aligned}\sigma_{\max}(G) &:= \max\{|S(C)| : C \in \mathcal{C}(G)\}, \\ \sigma_{\min}(G) &:= \min\{|S(C)| : C \in \mathcal{C}(G)\},\end{aligned}$$

and assuming that $C \in \mathcal{C}(G)$ is chosen randomly,

$$\sigma_{\text{rnd}}(G) := \mathbb{E}(|S(C)|).$$

Similarly, labeling each (directed) edge $(g_1, g_2) \in C$ with the difference $g_2 - g_1$, consider the set $D(C) \subseteq G$ of all labels along C and let

$$\begin{aligned}\delta_{\max}(G) &:= \max\{|D(C)| : C \in \mathcal{C}(G)\}, \\ \delta_{\min}(G) &:= \min\{|D(C)| : C \in \mathcal{C}(G)\},\end{aligned}$$

and (choosing $C \in \mathcal{C}(G)$ at random),

$$\delta_{\text{rnd}}(G) := \mathbb{E}(|D(C)|).$$

In this paper we find the exact values or establish tight bounds for these six quantities, for all finite abelian groups G .

We assume that $\min \emptyset = \max \emptyset = 0$ in the definitions above; thus, if G is trivial, then $\sigma_{\max}(G) = \sigma_{\min}(G) = \delta_{\max}(G) = \delta_{\min}(G) = 0$, while $\sigma_{\text{rnd}}(G)$ and $\delta_{\text{rnd}}(G)$ are undefined. Also, if $|G| = 2$, then $\sigma_{\max}(G) = \sigma_{\min}(G) = \delta_{\max}(G) = \delta_{\min}(G) = \sigma_{\text{rnd}}(G) = \delta_{\text{rnd}}(G) = 1$.

Occasionally, we will consider Hamiltonian cycles on *subsets* of finite abelian groups, as well as Hamiltonian *paths* on finite abelian groups or their subsets. The definitions of $S(C)$ and $D(C)$ are carried without any modification onto the case where C is a Hamiltonian cycle or path on a finite subset of an additively written group.

In connection with the quantities $\sigma_{\max}(G)$ and $\delta_{\max}(G)$ we will be interested in Hamiltonian cycles and paths such that all sums (differences) of two consecutive elements along the cycle or path are pairwise distinct; that is, $|S(C)| = |A|$ (respectively, $|D(C)| = |A|$) for a cycle and $|S(C)| = |A| - 1$ (respectively, $|D(C)| = |A| - 1$) for a path on the set A . We call such cycles and paths *rainbow-sum* (respectively, *rainbow-difference*) and use abbreviations like “RS-cycle” or “RD-path”. Under various names such cycles and paths have been studied by a number of authors; for details and references see next section and also comments at the end of Sections 4 and 7.

Both cycles and paths on the set A will be written as $C = (a_1, \dots, a_{|A|})$, where the components of C list the elements of A ; clearly, each Hamiltonian path on A has a unique representation of this sort, and each cycle has $|A|$ representations.

We close this section with the list of notation, used below in this paper and not introduced yet:

- $\langle g \rangle$ – the subgroup, generated by the group element g ;
- $\Sigma(G)$ – the sum of the elements of the finite abelian group G ;
- $\text{rk}(G)$ – the rank of the finite abelian group G ;
- $\mathbb{Z}/m\mathbb{Z}$ – the group of residues modulo the positive integer m ;
- $\text{Cay}_G^+(S)$ – the addition Cayley graph, induced on the finite abelian group G by its subset S (see next section for the definition).

2. SUMMARY OF RESULTS

We now briefly discuss our principal results; proofs (mostly of combinatorial nature), comments, and more results are postponed until Sections 3–8.

The smallest possible number of differences along a Hamiltonian cycle can be determined precisely.

Theorem 1. *For any finite abelian group G we have $\delta_{\min}(G) = \text{rk}(G)$.*

The situation with the *largest* possible number of differences is subtler and for some groups there is still room for improvement.

Theorem 2. *For any finite non-trivial abelian group G we have*

$$\delta_{\max}(G) \leq \begin{cases} |G| - 1 & \text{if } \Sigma(G) \neq 0; \\ |G| - 2 & \text{if } \Sigma(G) = 0. \end{cases}$$

Indeed, if G is not isomorphic to the direct sum of a group of odd order and a non-cyclic group of order 8, then equality is attained.

Notice, that the condition $\Sigma(G) \neq 0$ means that G has exactly one involution; equivalently, G has exactly one invariant factor of even order.

The proof of Theorem 2 uses results of Gordon [G61] and Headley [H94] asserting that (i) if $\Sigma(G) \neq 0$, then G possesses an RD-path; (ii) if $\Sigma(G) = 0$ and Sylow 2-subgroup of G is not of order 8, then the set of non-zero elements of G possesses an RD-cycle. (These results are based on earlier work of Friedlander, Gordon, and Miller [FGM78]). The question of whether the condition $\Sigma(G) = 0$ alone, without any extra assumptions, ensures the existence of an RD-cycle on the set of non-zero elements of G , to our knowledge is open. Answering it in the affirmative would show that in the estimate of Theorem 2 equality is actually attained for *all* finite non-trivial abelian groups G .

For those exceptional groups, not covered by the second assertion of Theorem 2, a lower bound for $\delta_{\max}(G)$ is immediate from our next result.

Theorem 3. *For any finite non-trivial abelian group G we have*

$$\delta_{\text{rnd}}(G) = (1 - e^{-1})|G| + O(1),$$

with an absolute implicit constant.

Observe that the expression $(1 - e^{-1})|G| + O(1)$ is not at all surprising in this context, giving the expected number of pairwise distinct elements of G , appearing in the sequence of $|G|$ randomly and independently chosen elements.

For a subset S of a finite abelian group G , consider the graph with the vertex set G and the edge set $\{(g', g'') \in G \times G : g' + g'' \in S\}$. We denote this graph by $\text{Cay}_G^+(S)$ and call it the *addition Cayley graph, induced on G by S* . Addition Cayley graphs received very little attention in the literature; we mention the papers [G61], where the clique number of the random addition Cayley graph is studied, and [CGW03], where Hamiltonicity of addition Cayley graphs is investigated in the special case that S does not contain elements of the form $2g$ with $g \in G$. The latter paper is particularly relevant in our context: in a somewhat unexpected way, it turns out

that the quantity $\sigma_{\min}(G)$ is tightly related to Hamiltonicity of the graphs $\text{Cay}_G^+(S)$. Specifically, if $C \in \mathcal{C}(G)$, then C is a Hamiltonian cycle in $\text{Cay}_G^+(S(C))$; conversely, if $S \subseteq G$ and C is a Hamiltonian cycle in $\text{Cay}_G^+(S)$, then $S(C) \subseteq S$. (We identify graphs with the digraphs, obtained by replacing each undirected edge with the pair of corresponding directed edges. Thus, for instance, if $|G| = 2$ and S contains the non-zero element of G , then $\text{Cay}_G^+(S)$ is considered Hamiltonian.) It follows that $\sigma_{\min}(G)$ is the minimum size of a subset $S \subseteq G$ such that $\text{Cay}_G^+(S)$ is Hamiltonian. We remark that Hamiltonicity of “conventional” Cayley graphs was intensively studied and in particular, it is well-known that any connected Cayley graph on a finite abelian group with at least three elements is Hamiltonian; see [M83]. However, apart from the results of [CGW03], nothing seems to be known on Hamiltonicity of *addition* Cayley graphs. We establish some properties of the graphs $\text{Cay}_G^+(S)$ in Section 6 and as a corollary determine the value of $\sigma_{\min}(G)$ precisely if G is of even order, and obtain reasonable estimates if G is of odd order.

Theorem 4. *Let G be a finite non-trivial abelian group. If $|G|$ is even and G is of type $(m_1, \dots, m_{\text{rk}(G)})$, then*

$$\sigma_{\min}(G) = \begin{cases} \text{rk}(G) & \text{if } m_1 = 2, \\ \text{rk}(G) + 1 & \text{if } m_1 > 2. \end{cases}$$

If $|G|$ is odd, then

$$\text{rk}(G) + 1 \leq \sigma_{\min}(G) \leq 2 \text{rk}(G) + 1.$$

Theorem 4 shows that $\sigma_{\min}(G) = 2$ if G is cyclic of even order $|G| \geq 4$, and $\sigma_{\min}(G) \in \{2, 3\}$ if G is cyclic of odd order. Indeed, we were able to find $\sigma_{\min}(G)$ for cyclic groups G of odd order, too.

Theorem 5. *If G is cyclic of order $|G| \geq 3$, then*

$$\sigma_{\min}(G) = \begin{cases} 2 & \text{if } |G| \text{ is even,} \\ 3 & \text{if } |G| \text{ is odd.} \end{cases}$$

Computations seem to suggest that if $\text{rk}(G) = 2$ and $|G| \neq 9$, then $\sigma_{\min}(G) = 3$. One can speculate that, indeed, $\sigma_{\min}(G) = \text{rk}(G) + 1$ for all non-cyclic finite abelian groups G of odd order, with a “small” number of exceptions.

Our next theorem establishes the largest possible number of sums along a Hamiltonian cycle.

Theorem 6. *For any finite non-trivial abelian group G we have*

$$\sigma_{\max}(G) = \begin{cases} |G| & \text{if } \Sigma(G) = 0 \text{ and } G \text{ is not} \\ & \text{an elementary abelian 2-group;} \\ |G| - 1 & \text{if } \Sigma(G) \neq 0; \\ |G| - 2 & \text{if } G \text{ is an elementary abelian} \\ & \text{2-group and } |G| > 2. \end{cases}$$

The proof of Theorem 6 is based on (i) a theorem due to Beals, Gallian, Headley, and Jungreis (see [BGHJ91]) claiming that if G is a finite abelian group with $\Sigma(G) = 0$, which is not an elementary 2-group, then G possesses an RS-cycle; (ii) a construction of an RS-path on every finite abelian group G with $\Sigma(G) \neq 0$.

It is worth mentioning that Theorem 6 bears relation with Latin transversals in Cayley tables, as we now explain. Let G be a finite abelian group. Does the Cayley table of G have a Latin transversal? In other words, do there exist two permutations $(g'_1, \dots, g'_{|G|})$ and $(g''_1, \dots, g''_{|G|})$ of the elements of G such that $(g'_1 + g''_1, \dots, g'_{|G|} + g''_{|G|})$ is also a permutation? It is easily seen that if the answer is positive, then $\Sigma(G) = 0$; on the other hand, it was shown in [P47] (see also [Su74] where this was independently rediscovered) that this condition is also sufficient. Notice the connection with Snevily's conjecture [Sn99], which is that any square sub-table of the Cayley table of a finite abelian group of odd order possesses a Latin transversal. Clearly, G has an RS-cycle if and only if its Cayley table has a Latin transversal of some special sort; namely, one with $g''_1 = g'_2, g''_2 = g'_3, \dots, g''_n = g'_1$.

Theorem 7. *For any finite non-trivial abelian group G we have*

$$\sigma_{\text{rnd}}(G) = (1 - e^{-1})|G| + O(1),$$

with an absolute implicit constant.

The reader is urged to compare Theorems 3 and 7.

3. THE MINIMUM NUMBER OF DIFFERENCES: $\delta_{\min}(G)$

Proof of Theorem 1. The case where G is trivial is immediate and we assume for the rest of the proof that $|G| \geq 2$.

Let $n := |G|$ and let $C = (g_1, \dots, g_n) \in \mathcal{C}(G)$ be a Hamiltonian cycle on G , written in such a way that $g_1 = 0$. In view of $g_{i+1} - g_i \in D(C)$ ($i = 1, \dots, n - 1$), every element of G can be represented as a sum of elements of $D(C)$; thus $D(C)$ generates G and consequently $|D(C)| \geq \text{rk}(G)$. It follows that $\delta_{\min}(G) \geq \text{rk}(G)$.

To show that $\delta_{\min}(G) \leq \text{rk}(G)$ we use induction by $\text{rk}(G)$. If $\text{rk}(G) = 1$ then G is cyclic and, identifying it with the group $\mathbb{Z}/n\mathbb{Z}$, we consider the Hamiltonian cycle

$C := (0, 1, 2, \dots, n - 1)$; clearly, $D(C) = \{1\}$, which settles the case $\text{rk}(G) = 1$. To complete the proof we show that for any Hamiltonian cycle $C = (h_1, \dots, h_n)$ on the n -element abelian group H and any integer $m \geq 2$, there is a Hamiltonian cycle C' on the group $H \oplus (\mathbb{Z}/m\mathbb{Z})$ with $|D(C')| \leq |D(C)| + 1$. Indeed, it is immediately verified that one can choose

$$\begin{aligned} C' := & (h_1, h_2, \dots, h_n, \\ & h_n + 1, h_1 + 1, \dots, h_{n-1} + 1, \\ & h_{n-1} + 2, h_n + 2, \dots, h_{n-2} + 2, \\ & \vdots \\ & h_2 + (m - 1), h_3 + (m - 1), \dots, h_1 + (m - 1)). \end{aligned}$$

□

4. THE MAXIMUM NUMBER OF DIFFERENCES: $\delta_{\max}(G)$

Proof of Theorem 2. Let $C = (g_1, \dots, g_{|G|}) \in \mathcal{C}(G)$. Since $0 \notin D(C)$, we have $|D(C)| \leq |G| - 1$. Moreover, if all non-zero elements of G are represented in $D(C)$, then exactly one of them, say g , is represented twice and therefore

$$0 = (g_2 - g_1) + \dots + (g_{|G|} - g_{|G|-1}) + (g_1 - g_{|G|}) = \Sigma(G) + g;$$

consequently, in this case $\Sigma(G) = -g \neq 0$. The first assertion of the theorem follows.

To prove the second assertion, notice first that if G is not isomorphic to the direct sum of a group of odd order and a non-cyclic group of order 8, then either $\Sigma(G) \neq 0$, or Sylow 2-subgroup of G is not of order 8. If $\Sigma(G) \neq 0$ then, as shown in [G61], the group G possesses an RD-path; closing this path (by joining its first and last elements), we get a Hamiltonian cycle $C \in \mathcal{C}(G)$ with $|D(C)| \geq |G| - 1$. If $\Sigma(G) = 0$ then G does not have an RD-path: otherwise, arguing as above we would obtain $\delta_{\max}(G) \geq |G| - 1$ which, as we saw, is wrong. It is shown in [H94], however, that if $\Sigma(G) = 0$ and Sylow 2-subgroup of G is not of order 8, then the set of non-zero elements of G possesses an RD-cycle. Choosing arbitrarily two adjacent elements of this cycle and inserting 0 between them, we obtain a Hamiltonian cycle $C \in \mathcal{C}(G)$ with $|D(C)| \geq |G| - 2$. □

For a survey of results, related to the existence of RD-path and RD-cycles in finite abelian groups, see [K96] or [O05]. We notice that the standard terminology used in [FGM78, H94, G61, K96, O05] and a number of other papers is distinct from that we use here. Specifically, RD-paths are called *directed terraces*, and those groups possessing an RD-path are called *sequenceable*; furthermore, RD-cycles on the set of

non-zero group elements are called *directed R-terraces*, and those groups for which such an RD-cycle exists are called *R-sequenceable*.

5. THE EXPECTED NUMBER OF DIFFERENCES: $\delta_{\text{rnd}}(G)$

Proof of Theorem 3. Let $n := |G|$; clearly, $n \geq 3$ can be assumed without loss of generality. Representing $D(C)$ as a sum of indicator random variables corresponding to the non-zero elements of G , write

$$\delta_{\text{rnd}}(G) = \sum_{g \in G \setminus \{0\}} \Pr \{g \in D(C)\} = \frac{1}{(n-1)!} \sum_{g \in G \setminus \{0\}} |\{C \in \mathcal{C}(G) : g \in D(C)\}|. \quad (1)$$

Assuming that $g \in G \setminus \{0\}$ is fixed, for each $A \subseteq G$ let $\mathcal{C}_A(G)$ denote the set of all cycles $C \in \mathcal{C}(G)$ such that every element $a \in A$ is followed along the cycle by the element $a + g$. Observe, that if A contains a coset of the subgroup $\langle g \rangle$, generated by g , then $\mathcal{C}_A(G)$ is empty, unless $A = \langle g \rangle = G$ (in which case $\mathcal{C}_A(G)$ consists of one single cycle, induced by g on G).

Claim 1. *If A does not contain a coset of $\langle g \rangle$, then $|\mathcal{C}_A(G)| = (n - |A| - 1)!$.*

Proof. For each $c \in G \setminus A$ find the non-negative integer k (depending on c) so that $c - (k+1)g \notin A$ and $c - kg, \dots, c - g \in A$. Consider all chains of the form $(c - kg, \dots, c - g, c)$, for all $c \in G \setminus A$. These chains partition G , and for $C \in \mathcal{C}(G)$ we have $C \in \mathcal{C}_A(G)$ if and only if C is composed of these chains, following each other in some order. The claim follows now since the number of chains is $|G \setminus A| = n - |A|$. \square

Using Claim 1 and the inclusion-exclusion principle, we get

$$\begin{aligned} |\{C \in \mathcal{C}(G) : g \in D(C)\}| &= \left| \bigcup_{A \subseteq G : |A|=1} \mathcal{C}_A(G) \right| \\ &= \sum_{\emptyset \neq A \subseteq G} (-1)^{|A|+1} |\mathcal{C}_A(G)| \\ &= \sum_{j=1}^{n-1} (-1)^{j+1} (n-j-1)! N_j + (-1)^{n+1} \tau, \end{aligned} \quad (2)$$

where N_j is the number of those $A \subseteq G$ with $|A| = j$ such that A contains no coset of $\langle g \rangle$, and τ equals 1 if $\langle g \rangle = G$ and equals 0 otherwise.

We now claim that if d is the order of g in G (so that $d \mid n$ and $d \geq 2$), then

$$N_j = \sum_{0 \leq i \leq j/d} (-1)^i \binom{n/d}{i} \binom{n-id}{j-id} \quad (3)$$

holds for each $j \in [1, n - 1]$. Indeed, represent G as a union of n/d cosets of $\langle g \rangle$. There are $\binom{n/d}{i}$ ways to choose i cosets, and for any choice of $i \leq j/d$ cosets there are $\binom{n-id}{j-id}$ ways to choose $j - id$ elements from the remaining cosets; our claim follows now by the inclusion-exclusion principle.

Substituting (2) and (3) into (1), and for $d \mid n$ letting K_d be the number of elements $g \in G$ of order d , we get

$$\begin{aligned} \delta_{\text{rnd}}(G) &= \frac{1}{(n-1)!} \sum_{d \mid n, d \geq 2} K_d \\ &\quad \times \left(\sum_{j=1}^{n-1} (-1)^{j+1} (n-j-1)! \sum_{0 \leq i \leq j/d} (-1)^i \binom{n/d}{i} \binom{n-id}{j-id} \right) + O(1) \\ &= \frac{1}{(n-1)!} \sum_{d \mid n, d \geq 2} K_d \\ &\quad \times \left(\sum_{0 \leq i \leq (n-1)/d} (-1)^i \binom{n/d}{i} (n-id)! \sum_{j=\max\{1,id\}}^{n-1} \frac{(-1)^{j+1}}{(j-id)!(n-j)} \right) + O(1) \\ &= M + R + O(1), \end{aligned}$$

where M is the part of the expression obtained for $i = 0$, and R is the remaining part (corresponding to positive values of i). The former is not difficult to compute:

$$\begin{aligned} M &= n \sum_{d \mid n, d \geq 2} K_d \sum_{j=1}^{n-1} \frac{(-1)^{j+1}}{j! (n-j)} \\ &= n \sum_{d \mid n, d \geq 2} K_d \sum_{j=1}^{n-1} \frac{(-1)^{j+1}}{j!} \left(\frac{1}{n} + O\left(\frac{j^2}{n^2}\right) \right) \\ &= \sum_{d \mid n, d \geq 2} K_d \left(1 - e^{-1} + O\left(\frac{1}{n}\right) \right) \\ &= (1 - e^{-1})n + O(1). \end{aligned}$$

To complete the proof it remains to estimate the remainder term R . Clearly, we have

$$|R| \leq \frac{1}{(n-1)!} \sum_{d \mid n, d \geq 2} K_d \sum_{1 \leq i < n/d} \binom{n/d}{i} (n-id)! \sum_{j=id}^{n-1} \frac{1}{(j-id)!(n-j)}.$$

Consider the internal sum. If $id \leq j \leq \min\{id + 2, n - 1\}$ then

$$\frac{1}{(j-id)!(n-j)} \leq \frac{1}{n-j} \leq \frac{3}{n-id},$$

while for $id + 3 \leq j + 1 \leq n - 1$ we have

$$\frac{(j - id)!(n - j)}{(j + 1 - id)!(n - j - 1)} = \frac{n - j}{(j + 1 - id)(n - j - 1)} \leq \frac{1}{3} \frac{n - j}{n - j - 1} \leq \frac{2}{3},$$

and hence

$$\sum_{j=id}^{n-1} \frac{1}{(j - id)!(n - j)} = O\left(\frac{1}{n - id}\right).$$

Thus

$$|R| \leq \frac{1}{(n - 1)!} \sum_{d|n, d \geq 2} K_d \sum_{1 \leq i < n/d} \binom{n/d}{i} (n - id - 1)!$$

and to estimate the sum over i we observe that the summand corresponding to $i = 1$ is $\frac{n}{d}(n - d - 1)!$, while for $2 \leq i + 1 < n/d$ we have

$$\begin{aligned} \frac{\binom{n/d}{i+1}(n - (i+1)d - 1)!}{\binom{n/d}{i}(n - id - 1)!} &= \frac{n/d - i}{i + 1} \cdot \frac{1}{(n - (i+1)d) \cdots (n - id - 1)} \\ &\leq \frac{1}{(i+1)d} \cdot \frac{n - id}{n - id - 1} \leq \frac{2}{(i+1)d} \leq \frac{1}{2}. \end{aligned}$$

It follows that

$$\sum_{1 \leq i < n/d} \binom{n/d}{i} (n - id - 1)! \leq \frac{2n}{d} (n - d - 1)! \leq n(n - 3)!$$

and therefore

$$|R| \leq \frac{n(n - 3)!}{(n - 1)!} \sum_{d|n, d \geq 2} K_d = O(1),$$

completing the proof. \square

6. THE MINIMUM NUMBER OF SUMS: $\sigma_{\min}(G)$

In this section we establish some general results on Hamiltonicity of addition Cayley graphs and as a corollary derive Theorems 4 and 5. It is worth reminding that we identify undirected graphs with the corresponding digraphs so that, for instance, the complete graph on two vertices is treated as Hamiltonian.

The trivial necessary condition for Hamiltonicity is connectedness.

Proposition 1. *Let S be a subset of the finite abelian group G . In order for $\text{Cay}_G^+(S)$ to be connected it is necessary and sufficient that one of the following conditions holds:*

- (i) *S is not contained in a coset of a proper subgroup of G ;*
- (ii) *S is contained in the non-zero coset of an index 2 subgroup of G , but not contained in any other coset.*

Proof. The cases where G is trivial and where S is empty are easy to check. Assuming that G is non-trivial and S is non-empty, let H be the smallest subgroup such that S is contained in a coset of H ; in other words H is the subgroup, generated by the difference set $S - S$. Observe now that the component of 0 in $\text{Cay}_G^+(S)$ consists of all those elements of G , representable as $s_1 - s_2 + s_3 - \cdots + (-1)^{k+1}s_k$ with $k \geq 0$ and $s_1, \dots, s_k \in S$; that is, this component is the set $H \cup (S + H)$. Thus $\text{Cay}_G^+(S)$ is connected if and only if either $H = G$, or H is a subgroup of index 2 and $S \subseteq G \setminus H$. \square

We remark that for the special case where S does not contain group elements of the form $2g$ ($g \in G$), the assertion of Proposition 1 is equivalent to [CGW03, Proposition 2.3].

In contrast with the “conventional” case, connectedness is not sufficient for Hamiltonicity of an addition Cayley graph. Say, if $S = \{s_1, s_2\} \subseteq \mathbb{Z}/n\mathbb{Z}$, where $n \geq 3$ is an integer and $s_1 - s_2$ is co-prime with n , then the corresponding graph is connected, but not Hamiltonian. This follows from the fact that there are elements $g \in G$ with either $2g = s_1$, or $2g = s_2$; such elements have just one neighbor in the graph. Moreover, it can be shown that if $n \equiv 3 \pmod{4}$, $G = \mathbb{Z}/n\mathbb{Z}$, and $S = \{0, 1, 3\} \subseteq G$, then $\text{Cay}_G^+(S)$ is 2-connected, but not Hamiltonian.

Corollary 1. *Let S be a subset of the finite abelian group G such that $\text{Cay}_G^+(S)$ is Hamiltonian. Then $|S| \geq \text{rk}(G)$ and moreover, if G is of type $(m_1, \dots, m_{\text{rk}(G)})$ with $m_1 > 2$, then indeed $|S| \geq \text{rk}(G) + 1$.*

Proof. Since $\text{Cay}_G^+(S)$ is Hamiltonian, it is connected, hence S is not contained in a proper subgroup of G by Proposition 1. It follows that S generates G and therefore $|S| \geq \text{rk}(G)$.

Assume now that $|S| = \text{rk}(G)$. Fix arbitrarily an element $s \in S$ and let H denote the subgroup of G , generated by $S - s$. Since $0 \in S - s$, we have $\text{rk}(H) \leq |S - s| - 1 = \text{rk}(G) - 1$ whence H is a *proper* subgroup. By Proposition 1 and in view of $S \subseteq s + H$, the index of H in G is 2, and $s \notin H$. Writing for brevity $r := \text{rk}(G)$, fix a generating subset $\{h_1, \dots, h_{r-1}\}$ of H . Since $2s \in H$, there are integers u_1, \dots, u_{r-1} such that $2s = u_1h_1 + \cdots + u_{r-1}h_{r-1}$. We now distinguish two cases.

Suppose first that there is an index $i \in [1, r-1]$ such that u_i and the order of h_i in H are of distinct parity. To simplify the notation suppose, furthermore, that $i = 1$. Find an integer t so that $(u_1 + 2t)h_1 = h_1$ and set $h'_1 := s + th_1$. We have then

$$2h'_1 = (u_1 + 2t)h_1 + u_2h_2 + \cdots + u_{r-1}h_{r-1}$$

and it follows that h_1 , and thus also s , are contained in the subgroup of G , generated by $h'_1, h_2, \dots, h_{r-1}$. We conclude that this subgroup is the whole group G and hence $\text{rk}(G) \leq r - 1$, a contradiction.

We have shown that for each $i \in [1, r-1]$, the order of h_i in H and u_i are of the same parity. One derives easily that there exists $h \in H$ such that $2s = 2h$ and then G is the direct sum of H and the two-element subgroup, generated by $s-h$. Consequently, $G \cong H \oplus (\mathbb{Z}/2\mathbb{Z})$ and since $\text{rk}(G) > \text{rk}(H)$, in the canonical representation of H all direct summands are of even order. Thus the canonical representation of G is obtained from that of H by adding $\mathbb{Z}/2\mathbb{Z}$ as a direct summand, meaning that $m_1 = 2$. \square

For groups of even order the estimate of Corollary 1 is sharp.

Lemma 1. *Let G be a finite abelian group of type $(m_1, \dots, m_{\text{rk}(G)})$. If $|G|$ is even, then there is a subset $S \subseteq G$ with*

$$|S| = \begin{cases} \text{rk}(G) & \text{if } m_1 = 2, \\ \text{rk}(G) + 1 & \text{if } m_1 > 2 \end{cases}$$

such that $\text{Cay}_G^+(S)$ is Hamiltonian.

Proof. Let $H < G$ be an index 2 subgroup with $\text{rk}(H) = \text{rk}(G) - 1$ if $m_1 = 2$, and $\text{rk}(H) = \text{rk}(G)$ if $m_1 > 2$. Fix an element $s \in G \setminus H$. By Theorem 1, there is a Hamiltonian cycle $C = (h_1, \dots, h_{|H|}) \in \mathcal{C}(H)$ such that $|D(C)| = \text{rk}(H)$. Now $C' := (h_1, s-h_1, h_2, s-h_2, \dots, h_{|H|}, s-h_{|H|})$ is a Hamiltonian cycle on G satisfying $|S(C')| = |D(C)| + 1$ and the assertion follows. \square

Lemma 2. *Let S be a finite non-trivial abelian group of odd order. Then there is a subset $S \subseteq G$ of size $|S| \leq 2\text{rk}(G) + 1$ such that $\text{Cay}_G^+(S)$ is Hamiltonian.*

Proof. We write $r := \text{rk}(G)$ and use induction by r . If $r = 1$ then G is cyclic and, identifying it with the group $\mathbb{Z}/(2n+1)\mathbb{Z}$ with a positive integer n , we consider the Hamiltonian cycle

$$C := (0, 1, 2n, 2, 2n-1, \dots, n, n+1) \in \mathcal{C}(G).$$

One verifies immediately that $|S(C)| = 3$, proving the lemma for $r = 1$.

Assuming now that $r \geq 2$, write $G = H \oplus F$ where H and F are subgroups of G such that $\text{rk}(H) = r - 1$ and F is cyclic. Write $|H| = m$ and $|F| = 2n + 1$ (so that $m \geq 3$ and $n \geq 1$ are integers) and find, using the induction hypothesis, a Hamiltonian cycle $C_H = (h_1, \dots, h_m) \in \mathcal{C}(H)$ such that $|S(C_H)| \leq 2r - 1$. Identifying F with the group $\mathbb{Z}/(2n+1)\mathbb{Z}$, consider the following $n+1$ paths in the complete

graph on the vertex set G :

$$\begin{aligned}
 & (h_1, \dots, h_m), \\
 & (h_1 + 1, h_2 + 2n, \dots, h_m + 1, h_1 + 2n, h_2 + 1, \dots, h_m + 2n), \\
 & \vdots \\
 & (h_1 + n, h_2 + (n+1), \dots, h_m + n, \\
 & \quad h_1 + (n+1), h_2 + n, \dots, h_m + (n+1)).
 \end{aligned}$$

Straightforward verification shows that the (cyclic) concatenation of these paths yields a Hamiltonian cycle $C \in \mathcal{C}(G)$ with $S(C) = S(C_H) \cup \{h_m + h_1 + 1, h_m + h_1 + (n+1)\}$. Thus $|S(C)| = |S(C_H)| + 2 \leq 2r + 1$ and the assertion follows. \square

Theorem 4 is immediate from Corollary 1, Lemmas 1 and 2, and the remark, preceding the statement of Theorem 4 in Section 2. To prove Theorem 5 we classify those subsets S of the finite abelian group G with $|S| \leq 2$ and such that $\text{Cay}_G^+(S)$ is Hamiltonian.

Lemma 3. *Let G be a finite abelian group with $|G| \geq 3$.*

- (i) *If $|S| = 1$ then $\text{Cay}_G^+(S)$ is not Hamiltonian;*
- (ii) *If $|S| = 2$ then $\text{Cay}_G^+(S)$ is Hamiltonian if and only if the difference of the two elements of S generates an index 2 subgroup of G , and this subgroup is disjoint with S .*

Proof. The first assertion is immediate; to prove the second assertion assume that $|S| = 2$ and write $n = |G|$ and $S = \{s_1, s_2\}$. If n is odd then there is an element $g \in G$ with $2g = s_1$; the vertex of $\text{Cay}_G^+(S)$, corresponding to g , has then just one neighbor, whence $\text{Cay}_G^+(S)$ is not Hamiltonian. Suppose that n is even. In this case for $\text{Cay}_G^+(S)$ to be Hamiltonian it is necessary and sufficient that in the n -element sequence

$$(0, s_1, s_2 - s_1, s_1 - (s_2 - s_1), 2(s_2 - s_1), \dots, s_1 - (n/2 - 1)(s_2 - s_1))$$

all elements are pairwise distinct and the last element equals s_2 . The latter condition means that the difference $s_2 - s_1$ has order $n/2$ in G , and the former condition reduces then to $G = \{0, s_1\} \oplus H$, where H is the subgroup, generated by $s_2 - s_1$. Equivalently, H is a subgroup of index 2, to which neither s_1 nor s_2 belong. \square

Corollary 2. *For any finite abelian group G with $|G| \geq 3$ we have $\sigma_{\min}(G) \geq 2$. Equality is attained in the last estimate if and only if G has a cyclic subgroup of index 2; that is, either G is cyclic of even order, or G is of type $(2, m)$ with an even $m \geq 2$.*

To complete our investigation of the quantity $\sigma_{\min}(G)$ we observe that for $|G|$ even the assertion of Theorem 5 follows from Corollary 2, or alternatively from the combination of Corollary 1 and Lemma 1; for $|G|$ odd it follows by combining Corollary 2 and Lemma 2.

7. THE MAXIMUM NUMBER OF SUMS: $\sigma_{\max}(G)$

Proof of Theorem 6. If $C = (g_1, \dots, g_{|G|})$ is an RS-cycle over the finite non-trivial abelian group G , then $\Sigma(G) = (g_1 + g_2) + \dots + (g_{|G|} + g_1) = 2\Sigma(G)$, whence $\Sigma(G) = 0$. Thus, if $\Sigma(G) \neq 0$ then $\sigma_{\max}(G) \leq |G| - 1$. Moreover, if G is an elementary abelian 2-group with $|G| > 2$, then by Theorem 2 we have $\sigma_{\max}(G) = \delta_{\max}(G) \leq |G| - 2$ and indeed, equality holds provided that $|G| > 2$ and $|G| \neq 8$. Furthermore, if G is elementary abelian of order $|G| = 8$, then a cycle $C \in \mathcal{C}(G)$ with $|S(C)| = 6$ is easy to construct; say, if g_1, g_2, g_3 are three independent elements of G , then one can set

$$C := (0, g_1, g_2, g_3, g_1 + g_2, g_1 + g_2 + g_3, g_1 + g_3, g_2 + g_3).$$

This establishes the upper bound for $\sigma_{\max}(G)$ and shows that equality is attained if G is an elementary abelian 2-group with $|G| > 2$.

If $\Sigma(G) = 0$ and G is not an elementary abelian 2-group, then by [BGHJ91, Theorem 6.6] the group G possesses an RS-cycle, which proves the assertion in this case.

Finally, suppose that $\Sigma(G) \neq 0$ and therefore G is the direct sum of a (possibly, trivial) group of odd order and a cyclic group of even order. Identifying the latter group with the corresponding group of residues, we can then write $G = H \oplus (\mathbb{Z}/n\mathbb{Z})$, where H is a group of odd order $k := |H|$, and $n = 2m$ is a positive even integer. If $k = 1$ we let $h_1 = 0$ (the zero element of the group H), if $k \geq 3$ we fix an RS-cycle $(h_1, \dots, h_k) \in \mathcal{C}(H)$; the existence of such an RS-cycle follows from $\Sigma(H) = 0$. Consider the Hamiltonian paths P' and P'' on $\mathbb{Z}/n\mathbb{Z}$ defined by

$$P' := (0, m, 1, m+1, 2, m+2, \dots, m-1, 2m-1),$$

$$P'' := (m, 0, m+1, 1, m+2, 2, \dots, 2m-1, m-1).$$

We have $S(P') = S(P'') = (\mathbb{Z}/n\mathbb{Z}) \setminus \{m-1\}$, so that P' and P'' are RS-paths. For $i = 1, \dots, n$ let p'_i and p''_i denote the i th elements of P' and P'' , respectively. Observing that $p'_n + p''_1 = p''_n + p'_1 = m-1$, one verifies easily that

$$\begin{aligned} P := & (h_1 + p'_1, h_1 + p'_2, \dots, h_1 + p'_n, \\ & h_2 + p''_1, h_2 + p''_2, \dots, h_2 + p''_n, \\ & \vdots \\ & h_k + p'_1, h_k + p'_2, \dots, h_k + p'_n) \end{aligned}$$

is a Hamiltonian path on G with $S(P) = G \setminus \{h_1 + h_k + (m - 1)\}$, hence an RS-path on G . Closing it (by joining its last and first elements) we obtain a Hamiltonian cycle $C \in \mathcal{C}(G)$ with $|S(C)| \geq |S(P)| = |G| - 1$, as wanted. \square

We note that RS-cycles were first introduced in [BGHJ91], where they are called *harmonious sequences* and those groups with an RS-cycle are called *harmonious groups*.

8. THE EXPECTED NUMBER OF SUMS: $\sigma_{\text{rnd}}(G)$

Proof of Theorem 7. Consider the two subgroups of the group G defined by $G_0 := \{g \in G: 2g = 0\}$ and $2G := \{2g: g \in G\}$. Let $n := |G|$ and $n_0 := |G_0|$, so that $|2G| = n/n_0$ in view of the isomorphism $G/G_0 \cong 2G$. Without loss of generality we assume that $n \geq 3$.

Given a Hamiltonian cycle $C \in \mathcal{C}(G)$, represent $S(C)$ as a sum of indicator random variables corresponding to the elements of G , and write

$$\sigma_{\text{rnd}}(G) = \sum_{g \in G} \Pr \{g \in S(C)\} = \frac{1}{(n-1)!} \sum_{g \in G} |\{C \in \mathcal{C}(G): g \in S(C)\}|. \quad (4)$$

Assuming that $g \in G$ is fixed, for each $A \subseteq G$ let $\mathcal{C}_A(G)$ denote the set of all cycles $C \in \mathcal{C}(G)$ such that every $a \in A$ is followed along C by $g - a$. Observe, that if $g = a' + a''$ with some $a', a'' \in A$, then a' is to be followed by a'' and vice versa along any cycle $C \in \mathcal{C}_A(G)$; consequently, $\mathcal{C}_A(G)$ is empty in this case. On the other hand, if g has no representations as $g = a' + a''$ with $a', a'' \in A$, then it is easy to see that $|\mathcal{C}_A(G)| = (n - |A| - 1)!$ (compare with Claim 1 in the proof of Theorem 3). Using the inclusion-exclusion principle we get

$$\begin{aligned} |\{C \in \mathcal{C}(G): g \in S(C)\}| &= \left| \bigcup_{A \subseteq G: |A|=1} \mathcal{C}_A(G) \right| \\ &= \sum_{\emptyset \neq A \subseteq G} (-1)^{|A|+1} |\mathcal{C}_A(G)| \\ &= \sum_{j=1}^{n-1} (-1)^{j+1} (n-j-1)! N_j, \end{aligned} \quad (5)$$

where N_j is the number of those $A \subseteq G$ with $|A| = j$ such that g cannot be represented as indicated above.

If $g \notin 2G$ then G is a disjoint union of pairs of the form $(c, g - c)$ with $c \in G$, and in order for A to have the property that $a' + a'' \neq g$ for all $a', a'' \in A$, it is necessary and sufficient that A contains at most one element out of each pair. Thus, $N_j = \binom{n/2}{j} 2^j$ if $j \leq n/2$, and $N_j = 0$ if $j > n/2$ in this case. On the other hand, if $g \in 2G$ then there

are n_0 representations $g = 2c$ with $c \in G$; removing such elements c from G , we can split the remaining $n - n_0$ elements into $(n - n_0)/2$ pairs as above, and now in order for A to have the property in question it is necessary and sufficient that A contains at most one element out of each of these pairs (and no non-paired elements). Therefore, in this case $N_j = \binom{(n-n_0)/2}{j} 2^j$ if $j \leq (n - n_0)/2$, and $N_j = 0$ if $j > (n - n_0)/2$. Using these observations, from (4) and (5) we obtain

$$\begin{aligned} \sigma_{\text{rnd}}(G) &= \frac{1}{(n-1)!} \left(1 - \frac{1}{n_0}\right) n \sum_{1 \leq j \leq n/2} (-1)^{j+1} (n-j-1)! \binom{n/2}{j} 2^j \\ &\quad + \frac{1}{(n-1)!} \frac{n}{n_0} \sum_{1 \leq j \leq (n-n_0)/2} (-1)^{j+1} (n-j-1)! \binom{(n-n_0)/2}{j} 2^j, \end{aligned} \quad (6)$$

where the first summand is to be dropped if n is odd.

Let now m denote one of the numbers $n/2$ and $(n - n_0)/2$ and suppose that m is an integer. Notice that for any $j \in [1, m]$ we have

$$\frac{1}{(n-1)!} (n-j-1)! = \frac{1}{(n-j) \cdots (n-1)} > n^{-j}$$

while, on the other hand,

$$\begin{aligned} \frac{1}{(n-1)!} (n-j-1)! &= n^{-j} \left(1 - \frac{1}{n}\right)^{-1} \cdots \left(1 - \frac{j}{n}\right)^{-1} \\ &< n^{-j} e^{2(\frac{1}{n} + \cdots + \frac{j}{n})} \leq n^{-j} e^{2j^2/n} < n^{-j} (1 + O(j^2/n)). \end{aligned}$$

It follows that

$$\begin{aligned} \frac{1}{(n-1)!} \sum_{j=1}^m (-1)^{j+1} (n-j-1)! \binom{m}{j} 2^j &= - \sum_{j=1}^m \binom{m}{j} \left(-\frac{2}{n}\right)^j + O\left(\frac{1}{n} \sum_{j=1}^m \binom{m}{j} j^2 \left(\frac{2}{n}\right)^j\right) \\ &= 1 - \left(1 - \frac{2}{n}\right)^m + O\left(\frac{1}{n} \sum_{j=1}^m \frac{j^2}{j!} \left(\frac{2m}{n}\right)^j\right) \\ &= 1 - e^{m \ln(1-2/n)} + O\left(\frac{1}{n} \sum_{j=1}^m \frac{j^2}{j!}\right) \\ &= 1 - e^{-2m/n + O(m/n^2)} + O(1/n) \\ &= 1 - e^{-2m/n} (1 + O(m/n^2)) + O(1/n) \\ &= 1 - e^{-2m/n} + O(1/n). \end{aligned}$$

Now if n is odd then $n_0 = 1$ and (6) along with the last computation give

$$\sigma_{\text{rnd}}(G) = n \left(1 - e^{-(n-1)/n} + O(1/n) \right) = (1 - e^{-1}) n + O(1),$$

as wanted. Similarly, if n is even then

$$\begin{aligned} \sigma_{\text{rnd}}(G) &= \left(1 - \frac{1}{n_0} \right) n \left(1 - e^{-1} + O(1/n) \right) + \frac{n}{n_0} \left(1 - e^{-(n-n_0)/n} + O(1/n) \right) \\ &= (1 - e^{-1}) n + \frac{n}{n_0} \left(e^{-1} - e^{-(n-n_0)/n} \right) + O(1) \\ &= (1 - e^{-1}) n + \frac{1 - e^{n_0/n}}{n_0/n} e^{-1} + O(1) \\ &= (1 - e^{-1}) n + O(1), \end{aligned}$$

completing the proof. \square

REFERENCES

- [BGHJ91] R. BEALS, J.A. GALLIAN, P. HEADLEY, and D. JUNGREIS, Harmonious groups, *J. Comb. Theory, Series A* **56** (1991), 223–238.
- [CGW03] B. CHEYNE, V. GUPTA, and C. WHEELER, Hamilton Cycles in Addition Graphs, *Rose-Hulman Undergraduate Math. Journal* **1** (4) (2003) (electronic).
- [FGM78] R.J. FRIEDLANDER, B. GORDON, and M.D. MILLER, On a group sequencing problem of Ringel, *Congr. Numer.* **21** (1978), 307–321.
- [G61] B. GORDON, Sequences in groups with distinct partial products, *Pacific J. Math.* **11** (1961), 1309–1313.
- [G05] B. GREEN, Counting sets with small sumset, and the clique number of random Cayley graphs, *Combinatorica* **25** (3) (2005), 307–326.
- [H94] P. HEADLEY, R-sequenceability and R*-sequenceability of Abelian 2-groups, *Discrete Math.* **131** (1–3) (1994), 345–350.
- [K96] A.D. KEEDWELL, Complete mappings and sequencings of finite groups, in *CRC Handbook of Combinatorial Designs* (C.J Colbourn and J.H Dinitz eds.), CRC Press 1996, 246–253.
- [M83] D. MARUŠIČ, Hamiltonian circuits in Cayley graphs, *Discrete Math.* **46** (1) (1983), 49–54.
- [O05] M.A. OLLIS, On terraces for abelian groups, *Discrete Mathematics* **305** (2005), 250–263.
- [P47] L.J. PAIGE, A note on finite Abelian groups, *Bull. Amer. Math. Soc.* **53** (1947), 590–593.
- [P51] ———, Complete mappings of finite groups, *Pacific J. Math.* **1** (1951), 111–116.
- [Sn99] H.S. SNEVILY, Unsolved Problems: The Cayley Addition Table of \mathbb{Z}_n , *Amer. Math. Monthly* **106** (6) (1999), 584–585.
- [Su74] J. SURÁNYI, A certain way of presenting finite abelian groups [Hungarian], *Mat. Lapok* **23** (1972), 257–259 (1974).

DEPARTMENT OF MATHEMATICS, THE UNIVERSITY OF HAIFA AT ORANIM, TIVON 36006,
ISRAEL

E-mail address: seva@math.haifa.ac.il